REMARKS

The Office Action mailed on August 2, 2004, has been carefully reviewed and the foregoing amendments and following remarks are offered in response thereto. Applicants respectfully request favorable reconsideration of this application, as amended.

Claims 27 and 28 were rejected under 35 U.S.C. § 102(e) as being anticipated by Schneck (USP 6,314,409). Claims 29–45 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Schneck in view of Granger (USP 6,480,959). Without acceding to the rejection under 35 U.S.C. § 102(e), Claims 27 and 28 have been amended to clarify certain features of the claimed invention. Without acceding to the rejection under 35 U.S.C. § 103(a), Claims 33–44 have been amended to correct various informalities and to clarify certain features of the claimed invention. Claims 46 and 47 have been added. Thus, Claims 27–47 are pending.

Claim 27 is directed to a method for protecting one or more computer systems using the same secret key cryptographic algorithm and recites, *inter alia*, separating a standard cryptographic algorithm into a plurality of simultaneous calculation processes based on secret data, creating a plurality of partial intermediate variables corresponding to each intermediate variable of the standard cryptographic algorithm, applying nonlinear transformations to each of the plurality of partial intermediate variables to create a plurality of partial results and reconstituting a final result, corresponding to a result of the standard cryptographic algorithm, from the plurality of partial results. Claim 33, directed to a computer system, recites similar subject matter. Schneck, directed to a system for controlling access and distribution of digital property, fails to teach or suggest these features.

Schneck's digital access and distribution system 100 includes data distributor 102 and user 104. Using authoring mechanism 114, data distributor 102 produces packaged data 108, which includes various data encrypted using a data-encrypting key K_D. The data-encrypting key K_D is encrypted using a rule-encrypting key K_R and included within packaged data 108. *See*, e.g., Col. 9, lines 51–57; Col. 10, lines 47–54; Col. 12, lines 13–38, lines 39–60; FIGS. 1–4. Schneck fails to disclose separating a standard cryptographic algorithm into a plurality of simultaneous calculation processes based on secret data, as recited by Claims 27 and 33. Rather, in contrast to the Applicants' invention, Schneck teaches that a data-encryption algorithm is first selected based on various factors including risk, degree of protection, etc., and then the various elements of data 106 are simply encrypted using the

data encryption key K_D (as required). *See*, e.g., Col. 14, lines 39–53; Col. 12, line 61 to Col. 15, line 48).

Furthermore, Schneck is entirely silent on whether his system creates a plurality of partial intermediate variables corresponding to each intermediate variable of the standard cryptographic algorithm, as recited by Claims 27 and 33. Moreover, Schneck fails to teach or suggest applying nonlinear transformations to each of the plurality of partial intermediate variables to create a plurality of partial results and reconstituting a final result, corresponding to a result of the standard cryptographic algorithm, from the plurality of partial results, as recited by Claims 27 and 33. Granger, directed to a method for protecting software applications from unauthorized distribution and using an electronic security device, pseudo-code or obfuscation, fails to provide the subject matter missing from Schneck.

Claims 27 and 33 thus clearly distinguish patentably from Schneck and Granger. Moreover, none of the remaining references, taken either singly or in combination, teaches or suggests the aforementioned features of Claims 27 and 33.

In view of the amendments presented herein, and the reasons explained in the preceding remarks, Applicants submit that this application is in condition for allowance and should now be passed to issue. A Notice of Allowance is respectfully solicited.

If any extension of time is required in connection with the filing of this paper and has not been requested separately, such extension is hereby requested.

The Commissioner is hereby authorized to charge any fees and to credit any overpayments that may be required by this paper under 37 C.F.R. §§ 1.16 and 1.17 to Deposit Account No. 50-1165.

Respectfully submitted,

Miles & Stockbridge P.C.

November 2, 2004

By: _____

Edward J. Kondracki
Reg. No. 20,604

Adam M. Treiber
Reg. No. 48,000

1751 Pinnacle Drive, Suite 500
McLean, Virginia 22102

(703) 903-9000

#9231560v1